

Office of the Secretary of Defense

§ 310.4

SOURCE: 72 FR 18758, Apr. 13, 2007, unless otherwise noted.

Subpart A—DoD Policy

§ 310.1 Reissuance.

This part consolidates into a single location (32 CFR part 310) Department of Defense (DoD) policies and procedures for implementing the Privacy Act of 1974, as amended (5 U.S.C. 552a) by authorizing the development, publication and maintenance of the DoD Privacy Program set forth by DoD Directive 5400.11¹ and 5400.11-R,² both entitled: “DoD Privacy Program.”

§ 310.2 Purpose.

This part:

(a) Updates the established policies and assigned responsibilities of the DoD Privacy Program pursuant to 5 U.S.C. 552a (also known and referred to in this part as “The Privacy Act”) and Office of Management and Budget (OMB) Circular No. A-130.

(b) Authorizes the Defense Privacy Board and the Defense Data Integrity Board.

(c) Prescribes uniform procedures for implementation of and compliance with the DoD Privacy Program.

(d) Delegates authorities and responsibilities for the effective administration of the DoD Privacy Program.

[80 FR 4207, Jan. 27, 2015]

§ 310.3 Applicability and scope.

(a) This part applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this part as the “DoD Components”).

(b) For the purposes of subsection (i), “Criminal penalties,” of The Privacy Act, any DoD contractor and any employee of such a contractor will be considered to be an employee of DoD when

DoD provides by a contract for the operation by or on behalf of DoD of a system of records to accomplish a DoD function. DoD will, consistent with its authority, cause the requirements of section (m) of The Privacy Act to be applied to such systems.

[80 FR 4207, Jan. 27, 2015]

§ 310.4 Definitions.

The following definitions apply to this part:

Access. The review of a record or a copy of a record or parts thereof in a system of records by any individual.

Agency. For the purposes of disclosing records subject to the Privacy Act among the DoD Components, the Department of Defense is considered a single agency. For all other purposes to include requests for access and amendment, denial of access or amendment, appeals from denials, and record keeping as relating to release of records to non-DoD Agencies, each DoD Component is considered an agency within the meaning of the Privacy Act.

Breach. A loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information (PII), whether physical or electronic.

Computer matching. The computerized comparison of two or more automated systems of records or a system of records with non-federal records. Manual comparisons are not covered.

Confidential source. A person or organization who has furnished information to the Federal Government under an express promise, if made on or after September 27, 1975, that the person’s or the organization’s identity shall be held in confidence or under an implied promise of such confidentiality if this implied promise was made on or before September 26, 1975.

Disclosure. The information sharing or transfer of any PII from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, government agency, or private entity other than the subject of the

¹Copies may be obtained at <http://www.dtic.mil/whs/directives>.

²See footnote 1 to § 310.1.